REGULAMIN OCHRONY DANYCH OSOBOWYCH W FUNDACJI WIDZEWA

SIEDZIBA FUNDACJI:
al. Marszałka Józefa Piłsudskiego 138, 92-230 Łódź

LOKALIZACJA, POD KTÓRĄ REALIZOWANE SĄ CZYNNOŚCI ADMINISTRACYJNE DLA FUNDACJI WIDZEWA (MIEJSCE PRZETWARZANIA DANYCH) - (FORUM 76):
al. Marszałka Józefa Piłsudskiego 76, 90-330 Łódź

Na podstawie art. 24 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku

z Przetwarzaniem Danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne Rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), uznając, że jest to proporcjonalne w stosunku do czynności przetwarzania, wdraża się do stosowania niniejszy Regulamin Ochrony Danych Osobowych.

Niniejszy Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Fundacji Widzewa:

1. Pracowników,
2. Współpracowników,
3. Podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora Danych Fundacji Widzewa.

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się w szczególności: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety, smartfony i inne telekomunikacyjne końcowe nośniki danych.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wgląd do danych wyświetlanych na monitorach komputerowych – **Polityka czystego ekranu.**

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego - następnie wyłączyć sprzęt komputerowy,
   b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki, na których znajdują się dane osobowe.
7. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive).
8. Użytkownicy komputerów przenośnych lub innych telekomunikacyjnych końcowych nośników danych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez internet zobowiązani są do stosowania zasad bezpieczeństwa.

I. ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik z dostępem do danych osobowych (np. na komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator - login.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji, na polecenie przełożonych.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie pracy innym osobom na koncie innego użytkownika.

II. POLISTYKA HASEŁ

1. Hasła powinny składać się z minimum 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy, jako haseł, wykorzystywać: dat, imion i nazwisk osób

bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.

4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, naklejać na monitorze komputera, trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Hasła powinny być zmieniane co 30-60 dni. Zmiany hasła dokonuje użytkownik.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

III. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnione osoby, pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach.
4. Zabrania się wyrzucania niezniszczonych dokumentów do koszy lub porzucania ich na zewnątrz np. na terenach publicznych.

IV. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora Danych.
2. Do takich nośników zalicza się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
3. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
4. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej.

5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest on do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

V. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na określoną stronę lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

VI. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania danych osobowych poza Związek należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w mailach nadawców bez weryfikacji tegoż nadawcy.
7. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
8. Należy zgłaszać informatykowi przypadki podejrzanych e-maili.
9. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
10. Użytkownicy powinni okresowo archiwizować oraz kasować niepotrzebne maile.
11. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
13. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
14. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

15. Użytkownik bez zgody Prezesa Fundacji nie ma prawa wysyłać wiadomości **zawierających dane osobowe** dotyczące Administratora Danych, jego pracowników czy kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

VII. OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np. Twój system jest zainfekowany, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

VIII. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia o każdym przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
   a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata, zagubienie danych),
c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów z danymi osobowymi, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b. dokumentacja jest masowo niszczona bez użycia niszczarki,
   c. fizyczna obecność w budynku lub pomieszczeniach osób nieupoważnionych do przebywania w Fundacji,
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia lub zgody Prezesa Fundacji,
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
   h. telefoniczne próby wyłudzenia danych osobowych,
   i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pendrive, innych nośników z danymi osobowymi,
   j. maile zachęcające do ujawnienia identyfikatora/hasła,
   k. pojawienie się wirusa komputerowego lub niestandardowe działanie komputerów,
   l. pozostawianie niezabezpieczonych haseł do systemów w pobliżu komputera, biurka.

IX. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,

b. zachowania w tajemnicy danych osobowych, do których ma lub będzie miała dostęp w związku z wykonywaniem zadań powierzonych przez Prezesa Fundacji,
c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Prezesa Fundacji,
d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem czy publikowaniem danych na stronach www.

2. Osoba dopuszczona do przetwarzania danych osobowych odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego **Regulaminu Ochrony Danych Osobowych** i przeszkolone, zobowiązane są podpisać **OŚWIADCZENIE O POUFNOŚCI**.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą statutową lub prawną dostępu do danych.

X. POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych, na podstawie Art. 107 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781 tj.).